



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/754,571	01/12/2004	Kensaku Yamaguchi	247558US2RD	8239
22850 7590 03/07/2007 OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C. 1940 DUKE STREET ALEXANDRIA, VA 22314			EXAMINER TURCHEN, JAMES R	
			ART UNIT	PAPER NUMBER
			2139	

SHORTENED STATUTORY PERIOD OF RESPONSE	NOTIFICATION DATE	DELIVERY MODE
3 MONTHS	03/07/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 03/07/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary

Application No.

10/754,571

Applicant(s)

YAMAGUCHI ET AL.

Examiner

James Turchen

Art Unit

2139

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 12 January 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-8 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-8 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 01/12/2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date See Continuation Sheet.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :04/12/2004, 11/08/2004, 12/20/2004, 05/18/2005, 08/30/2006.

DETAILED ACTION

1. Claims 1-8 are pending.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-8 are rejected under 35 U.S.C. 102(b) as being anticipated by Shirakawa et al. (US 2002/0051536).

Regarding claim 1:

Shirakawa et al. discloses a decryption unit (Figure 1, 501 and 601) configured to read out an execution code (501 reads out an instruction, paragraph 0040) or data (601 reads out data, paragraph 0040) of an encrypted program and decrypt the execution code or data (paragraph 0040) by using a prescribed encryption key, according to a decryption request from the cache memory control unit (paragraph 0041). It is inherent that a cache memory control unit or a memory management unit would issue a command to read or write from the cache. Shirakawa et al. discloses a cache memory (Figure 1, 301 and 401) configured to store the execution code or data decrypted by the decryption unit (Figure 1, 501 and 601) into one of the cache lines provided in cache memory, each cache line having a secret protection attribute holding section (Figures 7 and 8, "Key Pair Tag") for storing an actual encryption key used in decrypting the execution code or data; and a cache memory control unit (Figures 9 and 10, 504 and

Art Unit: 2139

604 respectively) configured to process a reading request for the execution code (paragraphs 74 and 75) or data (paragraphs 77 and 78) such that, if the execution code or data exists in the cache memory and the execution code or data in the cache memory is decrypted by an identical encryption key as the prescribed encryption key, the execution code or data in the cache memory is read out (It is inherent that the keys must match else random, garbled information will be read out).

Regarding claim 2:

Shirakawa et al. further discloses a key value register (Figure 4, 210) configured to store a desired encryption key to be used in decrypting the execution code or data, which is updated at each occasion of executing the encrypted program (It is an inherent property of cache to update after each occasion of executing); the cache memory control unit judges whether the execution code or data in the cache memory is decrypted by an identical encryption key as the prescribed encryption key, by comparing the desired encryption key stored in the key value register and the actual encryption key stored in the secret protection attribute holding section of a cache line for the execution code or data to be executed to see if two encryption keys are identical or not (paragraphs 0058-0064).

Regarding claim 3:

Shirakawa et al. discloses that the cache memory stores data decrypted by the decryption unit (Figures 2 and 3), and the cache memory control unit writes a processing result of the data into the cache, while storing the desired encryption key stored in the key value register into the secret protection holding attribute holding

Art Unit: 2139

section of a cache line for the data (paragraphs 0065-0067 disclose the EX/MEM stage of the pipeline wherein the core would write to the cache memory).

Regarding claim 4:

Shirakawa et al. discloses the cache memory stores data decrypted by the decryption unit, and the cache memory control unit encrypts a processing result of the data by using the actual encryption key stored in the secret protection attribute holding section of a cache line for the data, and writes encrypted data into an external memory device (paragraphs 0081 and 0082).

Regarding claims 5-8:

Claims 5-8 teach the method associated with the system discloses in the rejection of claims 1-4.

Conclusion

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The prior art discloses tamper-resistant microprocessors and cache.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Turchen whose telephone number is 571-270-1378. The examiner can normally be reached on MTWRF 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Walt Griffin can be reached on 571-272-1447. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2139

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JRT

Taghi J. Arani
Primary Examiner
Taghi J. Arani
3/11/07